



Vuelva a Tener el Control: Aumente la Seguridad, Empodere a los Empleados, Proteja el Negocio

Application Control White Paper

Octubre 2010

Introducción: Balanceando Productividad y Seguridad

Así como los trabajadores encuentran nuevas y creativas maneras de utilizar la red, las organizaciones se esfuerzan por mantener el control de la red corporativa mientras empoderan a los empleados, socios de negocios y otros interesados con acceso a funcionalidades críticas. Una asombrosa cantidad de nuevas aplicaciones han emergido y su número aumenta diariamente. El asunto empieza a ser complicado por el hecho de que considerar una aplicación como "buena" o "mala" ya no es una cuestión tan sencilla. Algunas aplicaciones están destinadas únicamente con propósitos del negocio y son cuidadosamente diseñadas para minimizar los riesgos de seguridad y maximizar la productividad. Del otro lado encontramos el riesgo de aplicaciones programadas para robar información, corromper computadores o interrumpir la actividad de la red. Una gran variedad de aplicaciones caen en esta área gris entre estos dos extremos.

La Evolución de las Aplicaciones Complica la Seguridad

Anteriormente los administradores de IT eran capaces de negar el acceso a aplicaciones cuyos orígenes se encontraban en el mercado de consumo, este acercamiento se está haciendo cada vez más complicado. Aplicaciones como Facebook han demostrado ser valiosas en las empresas, particularmente en los grupos de ventas y mercadeo. De hecho, 1,5 millones de empresas tienen páginas activas en Facebook. (Para información adicional y algunos otros hechos sobre Facebook, consulte <http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/>). De igual forma, los juegos en Facebook pueden acabar con la productividad y, si contienen malware, también generan un riesgo a la seguridad.

Esta evolución hace que los administradores deban reevaluar cómo configurar sus firewalls para proteger el ambiente corporativo. Algunos años atrás los administradores podían negar el acceso a las aplicaciones, definiendo políticas de firewall para bloquear ciertos puertos o protocolos. Pero dado que las aplicaciones hoy en día se presentan como tráfico web sobre el puerto 80 o el 443, este acercamiento ya no es suficiente o

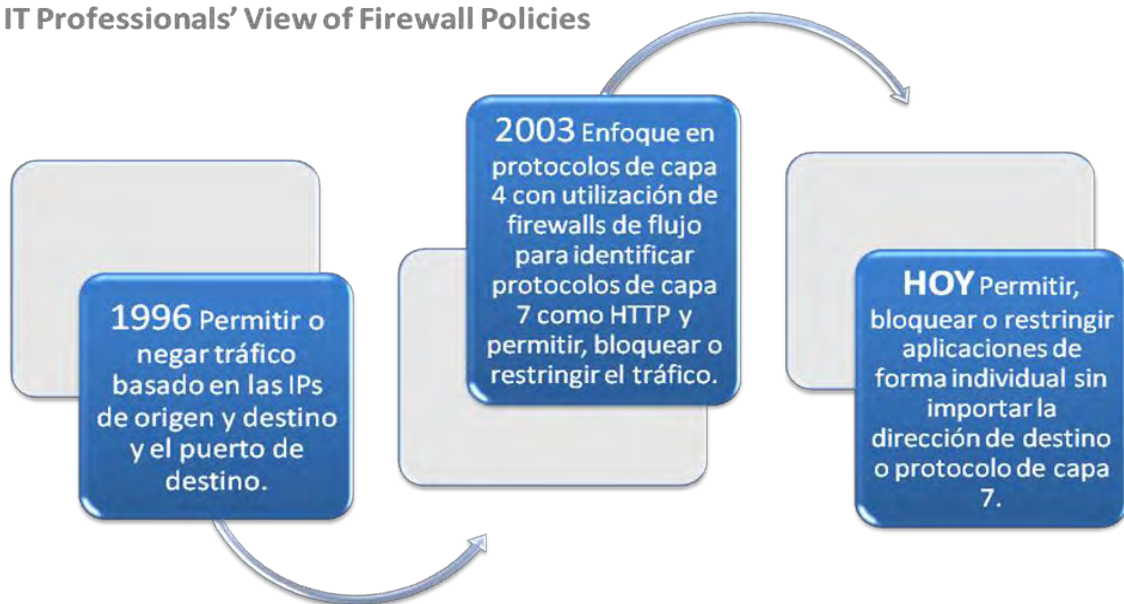
efectivo. Como resultado, los administradores han perdido mucho poder de control sobre las aplicaciones que se ejecutan en la organización.

Aplicaciones de mensajería instantánea (IM) o de peer-to-peer (P2P) son los principales ejemplos del por qué son necesarios nuevos niveles de control. La primera generación de estas aplicaciones podía ser regulada por medio de un acceso básico a las Listas de Control de Acceso (ACL), basadas en puertos de destino fijos o limitados y servidores de registro fácilmente identificables. Las aplicaciones de segunda generación utilizaban puertos dinámicos y servidores de registro que cambiaban sus direcciones frecuentemente o que tenían espejos tan extendidos que hacían las ACLs menos efectivas para bloquear las aplicaciones. La actual generación de aplicaciones de mensajería instantánea y peer-to-peer generalmente actúa como tráfico web y, en algunos casos, no requieren servidores de registro. Como resultado, son cada vez más eficientes para evadir los firewalls. De hecho, algunas aplicaciones (incluyendo UltraSurf, Skype y Winny) evaden el diseño de múltiples tecnologías de seguridad. Sin duda, las organizaciones necesitan un fuerte control de acceso a estas aplicaciones, especialmente aquellas que se encuentran sujetas a determinada regulación.

Los Administradores de IT Necesitan Retomar el Control

La siguiente línea de tiempo ayuda a ilustrar qué capacidades buscan los profesionales en seguridad en una solución.

IT Professionals' View of Firewall Policies



Para asegurar los ambientes corporativos de hoy, los administradores necesitan identificar y determinar si las aplicaciones son utilizadas para los fines de la empresa, son malware o caen dentro de la zona gris entre ellas. En este último caso, los profesionales IT necesitan la habilidad de controlar quién puede acceder a qué aplicaciones y con qué propósito. Aplicaciones web 2.0 como el streaming de medios o de audio pueden consumir grandes cantidades del costoso ancho de banda corporativo. Además, las organizaciones que se encuentran dentro de industrias reguladas deben restringir la utilización de servicios de mensajería instantánea ya que no cumplirían con los requerimientos para la retención de mensajes electrónicos. Como parte de una posición de seguridad y conformidad con las regulaciones, una política corporativa de uso aceptable, o una combinación de estas dos, la organización debe controlar la utilización de un amplio rango de aplicaciones por parte de sus usuarios.

El Riesgo de Seguridad Planteado por las Aplicaciones

La red es el principal origen de las amenazas a la seguridad en las organizaciones de hoy y las aplicaciones web por lo general son el principal foco de los atacantes. Simultáneamente, las redes sociales se encuentran en un rápido crecimiento y nuevos sitios web 2.0 surgen por doquier. Los usuarios no saben cómo tener adecuados niveles de privacidad en estos sitios. Como resultado de todo esto, los hackers encuentran muy provechoso utilizar las redes sociales como plataforma de lanzamiento de ataques de ingeniería social contra los usuarios de una organización. Los usuarios tienden a confiar en un link que encuentran en un sitio cuando éste es provisto por una conexión en su red social, sin darse cuenta que estas cuentas pueden ser muy fácilmente copiadas o falsificadas.

Dado que el tráfico y las aplicaciones web son el origen de muchos riesgos de seguridad, los administradores IT pueden erradicar los vectores potenciales de amenaza limitando a sus usuarios de manera que solamente tengan acceso a las aplicaciones que sean necesarias a los propósitos de la organización.

WatchGuard Application Control

WatchGuard continuamente evoluciona sus soluciones para mantenerlas al día con los desafíos a los que se enfrentan las organizaciones, sin importar su tamaño. Los dispositivos WatchGuard XTM 11.4 (y superiores) incluyen capacidades de control de aplicaciones que empoderan a los administradores para ejercer un control granular sobre cientos de aplicaciones, entendiendo qué aplicaciones están siendo utilizadas y por quién.

Application Control de WatchGuard es una suscripción de seguridad totalmente integrada a los dispositivos WatchGuard XTM. Provee monitoreo y filtrado global o basado en políticas para más de 1.500 aplicaciones web y de negocio para una mejor productividad y seguridad mejorada. Los administradores pueden aplicar las políticas de uso aceptable a sus usuarios y grupos, por categoría, aplicación y sub-funciones de la aplicación. Por ejemplo, pueden definir una política que permite al departamento de mercadeo el acceso a Facebook pero no a los juegos dentro de Facebook.

Utilizando más de 2.300 firmas y técnicas avanzadas de análisis de comportamiento, Application Control también brinda al administrador una visibilidad histórica y en tiempo real de la utilización (o intento de utilización) de aplicaciones dentro de la red. Este nivel de control y visibilidad ayuda a la organización a reforzar las Políticas de Uso Aceptable de obligatorio cumplimiento por las regulaciones de la industria, reglamentación legal y política, objetivos y cultura organizacional y similares.

Cómo Funciona WatchGuard Application Control

En la herramienta de configuración de WatchGuard XTM, el administrador configura una política global u otras más granulares que cobijen a usuarios específicos, grupos, redes u otros criterios que determinen qué aplicaciones pueden o no utilizar. En tiempo real, el WatchGuard XTM con Application Control inspecciona el tráfico que atraviesa el dispositivo y determina qué aplicación genera el tráfico. La tecnología basada en firmas combinada con un motor que evalúa el comportamiento de las aplicaciones, habilita el dispositivo para identificar las aplicaciones con un alto grado de precisión. El dispositivo refuerza la política definida por el administrador y genera un log de las acciones para una posterior revisión. Los administradores podrán acceder

Los Peligros de la World Wide Web

40.000 sitios web son comprometidos cada semana, el 0,7% de los resultados de búsqueda en Google entregan sitios que han sido infectados por malware. Fuente: [Google Security Blog](#), Agosto de 25, 2009.

Los ataques contra las aplicaciones web constituyen más del 60% del total de intentos de ataque en Internet. Fuente: [SANS Top 10 Security Risks](#), Septiembre de 2009.

El 64% de la gente entrevistada por AVG, sigue los links provistos por miembros de su comunidad de miembros en las redes sociales y el 26% comparte archivos en las redes sociales. Fuente: AVG, Social Engineering: Hacking people, not machines, 2009.

al la interface gráfica de reportes para ver la utilización de aplicaciones ejecutadas por los usuarios (o los intentos de ejecución) u las aplicaciones más utilizadas en la organización.

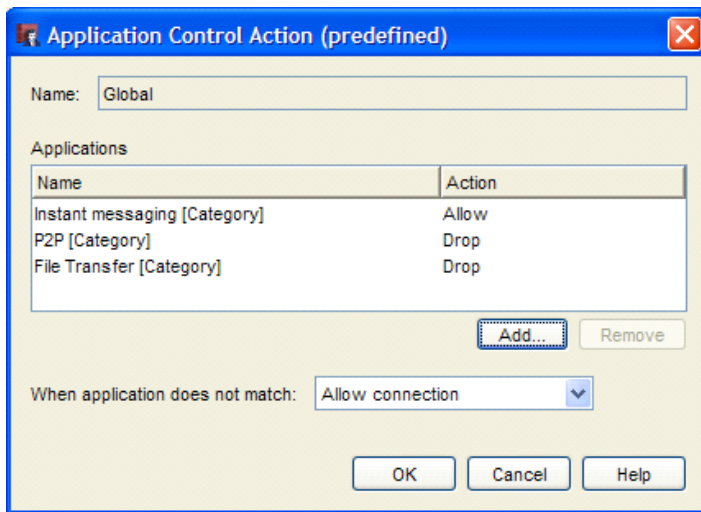


Figura 1: Los administradores pueden generar fácilmente la configuración de una política global para toda la red de la organización.

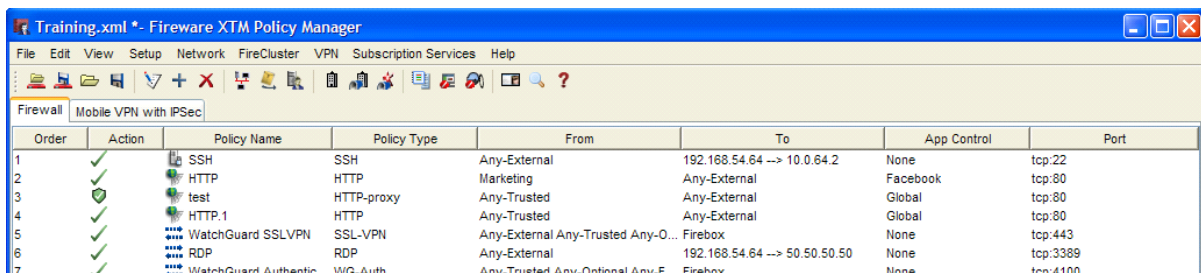


Figura 2: Los administradores pueden ejecutar un control granular sobre cientos de aplicaciones, organizadas por categoría, con la capacidad de controlar quién utiliza estas aplicaciones y cuándo lo hace.

Con WatchGuard Application Control las organizaciones pueden ejercer un control granular sobre la utilización de aplicaciones en la red corporativa. Por ejemplo:

- Bloquear la utilización de YouTube, Skype o QQ.
- Bloquear la utilización de todas las aplicaciones P2P a los usuarios que no hacen parte del grupo de gerencias.
- Permitir que el departamento de mercadeo tenga acceso a las redes sociales como Facebook o Twitter.
- Permitir la utilización de Windows Life Messenger para mensajería instantánea pero negar la transferencia de archivos sobre esta aplicación.
- Limitar la utilización de aplicaciones de streaming de medios a determinados horarios.
- Generar un reporte de las 10 aplicaciones más utilizadas en la organización
- Reportar la utilización (o intento) de aplicaciones por parte de cualquier individuo en la organización.

Qué Buscar en Application Control

Cuando se trata del control de aplicaciones, los siguientes criterios son muy importantes en la búsqueda de una solución:

- **Control Granular.** Para hacer frente a las diversas formas en que los usuarios pueden utilizar las aplicaciones, es importante controlar uno o más aspectos de una aplicación así como deshabilitar otras funciones de la misma. Por ejemplo, permitir la utilización de Windows Live Messenger para la mensajería instantánea pero bloquear la transferencia de archivos o, permitir el acceso a Facebook pero bloquear la ejecución de los juegos de Facebook.
- **Cantidad de firmas de aplicaciones.** Buscar una extensa lista de firmas que sea actualizada y mantenida en el tiempo por el fabricante. Nuevas aplicaciones se publican y el comportamiento de las aplicaciones cambia, las firmas deben ser actualizadas automáticamente sin requerir una actualización de la totalidad de los servicios de seguridad.
- **Capacidad de identificar aplicaciones cifradas.** La aplicaciones de hoy son programadas inteligentemente para tratar de sobrepasar las medidas de seguridad, cifrando la información y el tráfico de la aplicación al salir a Internet. La mejor solución utilizará análisis de comportamiento incluso para aplicaciones disfrazadas.
- **Incorporación en las políticas.** No es suficiente utilizar capacidades adicionales en un servicio de prevención de intrusiones para hacer frente a unas pocas aplicaciones. Busque una solución que permita al control de aplicaciones ser parte integral de las políticas básicas del firewall.
- **Balance de desempeño y eficacia.** Algunos productos que ofrecen control de aplicaciones requieren de un hardware costoso para entregar niveles aceptables de desempeño. La organización debe asegurarse de que sus productos de seguridad ofrezcan un alto rendimiento con un costo razonable además de la eficacia del control de aplicaciones que requieren.

Las Aplicaciones Basadas en Web Tienen un Alcance muy Amplio

Mensajería Instantánea

QQ, Windows Live Messenger, Yahoo! Messenger, GoogleTalk

Email

Hotmail, Gmail, Yahoo, Microsoft Exchange

Web 2.0

Facebook, LinkedIn, Twitter, Salesforce

Peer to Peer

Gnutella, Foxy, Winny, BitTorrent, eMule

Terminales de Acceso Remoto

TeamViewer, GoToMyPC, Webex

Base de Datos

Microsoft SQL, Oracle

Transferencia de Archivos

Peercast, Megaupload

Voz Sobre IP

Skype

Streaming de Medios

QuickTime, YouTube, Hulu

Administración de Red

Microsoft Update, Adobe, Norton, McAfee, Syslog

Entunelamiento (proxies de sobrepaso web)

Avoidr, Ultrasurf, Circumventor

Beneficios para los Administradores IT y la Organización

Al utilizar Application Control de WatchGuard las organizaciones encontrarán una gran variedad de beneficios. Adicionalmente a retomar el control del ambiente de red corporativo, los administradores IT tendrán más poder sobre las aplicaciones que el que tenían en el pasado. Como resultado podrán mantenerse al día con el siempre cambiante universo de las aplicaciones y satisfacer las demandas corporativas y de los usuarios. De hecho, aplicando políticas que controlan la utilización de aplicaciones los administradores aseguran que sus usuarios y otro personal puedan desempeñar sus funciones como es debido, que estén enfocados y sean productivos y eviten potenciales problemas legales asociados con el uso no autorizado de aplicaciones. Con un control completo de aplicaciones debidamente establecido, las organizaciones pueden estar seguras de que limitan los riesgos de seguridad y preservan el ancho de banda corporativo para una utilización consistente de las aplicaciones con objetivos corporativos.

WatchGuard XTM: Un Firewall con todas las Funciones para Control de Aplicaciones

Como empleados, socios de negocio y otros dentro del ambiente corporativo tienen acceso a una gran variedad de aplicaciones, las organizaciones deben encontrar la manera de balancear las necesidades de los usuarios con la seguridad. Ahora que tantas aplicaciones desafían una clara categorización, los administradores IT requieren nuevos niveles de control sobre las aplicaciones autorizadas y para quién lo están.

Este tipo de control de aplicaciones está disponible en los equipos WatchGuard XTM. WatchGuard lo distribuye como parte de su firewall integral, que incluye todas las funciones necesarias para de una forma fácil, comprensiva y costo eficiente, asegurar el ambiente corporativo. Adicionalmente a la configuración y refuerzo avanzados de políticas, XTM soporta todas las configuraciones básicas de puertos y protocolos que son familiares para los administradores además de características críticas de red que incluyen enrutamiento dinámico, conmutación de canales WAN y balanceo de cargas. Un método de arrastrar y soltar para VPNs hace muy fácil crear túneles sitio a sitio para conexiones seguras entre diferentes ubicaciones y además, un paquete interactivo de herramientas de monitoreo en tiempo real ahorran tiempo y hacen sencilla de ver la información sobre usuarios, redes y actividades de seguridad.

En la parte más alta de de la relación costo/rendimiento en la industria, WatchGuard XTM ofrece otras suscripciones de seguridad que entregan una completa capacidad de administración de las amenazas:

- **Reputation Enabled Defense:** Entrega un poderoso servicio de reputación en la nube que protege a los usuarios de páginas con contenido maligno mejorando impresionantemente el ancho de banda web.
- **spamBlocker:** Bloquea el email no deseado con casi un 100% de precisión así como las cargas de virus que el spam normalmente trae. spamBlocker reconoce el spam sin importar el idioma, formato o contenido del mensaje, así se trate de spam basado en imágenes que otros productos de anti-spam no logran detectar.
- **WebBlocker:** Un servicio de filtrado de contenido URL que bloquea el acceso a sitios peligrosos o inapropiados en el lugar de trabajo. Filtra el contenido en HTTP y cierra la brecha que otros filtros no logran filtrar sobre HTTPS.
- **Gateway AntiVirus:** Provee una poderosa protección basada en firmas en la puerta de enlace contra virus, trojanos, spyware y rogueware conocido.
- **Intrusion Prevention:** Explora todos los puertos y protocolos para bloquear ataques que puedan cumplir con el standard de los protocolos pero que carguen contenido maligno, incluyendo desbordamientos de buffer, inyección de SQL e inclusiones de archivos remotos.

Encuentre más sobre WatchGuard Application Control y la familia XTM de dispositivos de seguridad de red, visite www.watchguard.com, contacte a su vendedor local o llame a WatchGuard directamente al 1.800.734.9905 (Ventas U.S.A.) o +1.206.613.0895 (Ventas Internacionales).

DIRECCIÓN:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

PÁGINA WEB:
www.watchguard.com

VENTAS EN LOS EE. UU.:
1.800.734.9905

VENTAS INTERNACIONALES:
+1.206.613.0895

ACERCA DE WATCHGUARD

Desde 1996, WatchGuard Technologies provee dispositivos de seguridad confiables y fáciles de administrar a cientos de miles de organizaciones en todo el mundo. Las soluciones de seguridad para redes premiadas WatchGuard Extensible Threat Management (XTM) combinan firewall, VPN y servicios de seguridad. Los dispositivos Extensible Content Security (XCS) ofrecen seguridad de contenidos para correo electrónico y web así como Prevención de Pérdida de Información (DLP). Estas dos líneas de productos ayudan a satisfacer requisitos de conformidad como PCI DSS, HIPAA, SOX y GLBA. Más de 15000 socios de negocio representan a WatchGuard en 120 países. La sede principal de WatchGuard se encuentra en Seattle, Washington, USA y cuenta con oficinas en Norte América, Latino América, Europa, Asia y el Pacífico. Para más información por favor visite <http://www.watchguard.com/>

No se brindan garantías expresas ni implícitas. Todas las especificaciones están sujetas a cambios imprevistos y los productos, las características y las funciones previstas para el futuro se proveerán siempre y cuando estén disponibles. © 2010 WatchGuard Technologies, Inc. Todos los derechos reservados. WatchGuard, el logo de WatchGuard, Firebox y LiveSecurity son marcas comerciales o marcas registradas de WatchGuard Technologies, Inc. en los Estados Unidos y en otros países. Toda otra marca o nombre comercial es propiedad de sus respectivos dueños. Pieza n. ° WGCE66719_100410